PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2004-054488**
(43)Date of publication of application : **19.02.2004**

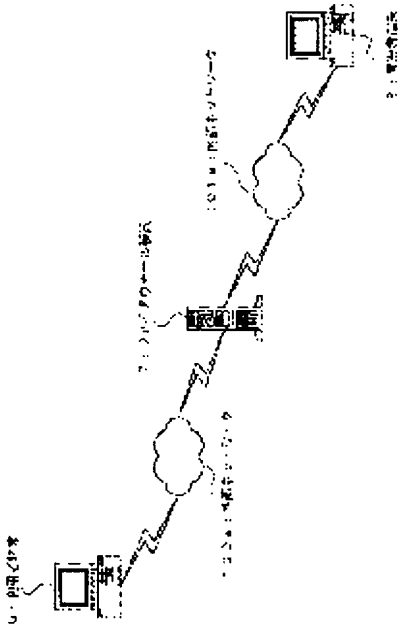
(51)Int.Cl. **G06F 13/00**
H04L 12/66

(21)Application number : **2002-209576**
(22)Date of filing : **18.07.2002**

(71)Applicant : **YOKOGAWA ELECTRIC CORP**
(72)Inventor : **ARAI TAKAYUKI**

(54) FIREWALL DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a firewall device capable of temporarily changing access limit without generating erroneous setting or security deterioration.
SOLUTION: This firewall device for limiting any illegal access to an internal network is provided with a firewall means connected to an external network for limiting any illegal access to the internal network, a setting interface means connected through the firewall means to an external network for fetching the changed contents of the setting of the firewall means, and a setting changing means for authenticating whether or not a user is preliminarily registered and authorized to use through the setting interface means, and for limiting the setting items settable for each authenticated user, and for changing the setting of the firewall means after evaluating the legality of the changed contents.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-54488
(P2004-54488A)
(43)公開日　平成16年2月19日(2004.2.19)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 13/00	G06F 13/00	351Z	5B089
H04L 12/66	H04L 12/66	B	5K030

審査請求 未請求　請求項の数 10　OL　（全 13 頁）

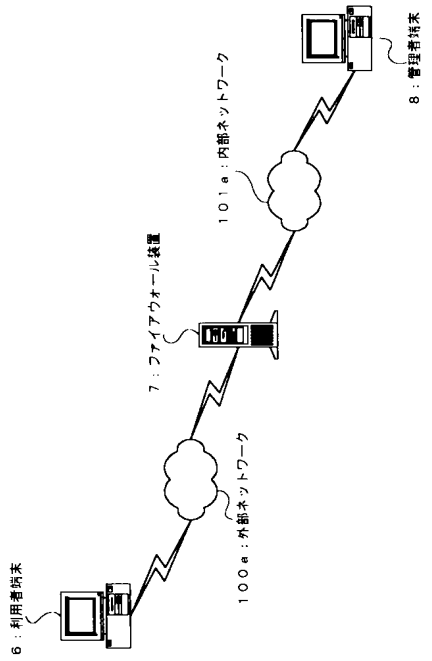
(21)出願番号　特願2002-209576(P2002-209576)
(22)出願日　平成14年7月18日(2002.7.18)

(71)出願人　000006507
横河電機株式会社
東京都武蔵野市中町２丁目９番３２号
(72)発明者　新井　貴之
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内

Fターム(参考)　5B089 GA04 GA11 JA32 KA17 KB13 KC14 KC52 KC58
5K030 GA15 HC01 HC13 HD03 HD06

(54)【発明の名称】ファイアウォール装置

(57)【要約】
【課題】誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能なファイアウォール装置を実現する。
【解決手段】内部ネットワークへの不正なアクセスを制限するファイアウォール装置において、内部ネットワークに対する不正なアクセスを制限する外部ネットワークに接続されたファイアウォール手段と、このファイアウォール手段を介して外部ネットワークに接続されファイアウォール手段の設定の変更内容を取り込む設定インターフェイス手段と、この設定インターフェイス手段を介して予め登録されている利用を許可された利用者であるかの認証をし、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性を評価した上でファイアウォール手段の設定を変更する設定変更手段とを設ける。
【選択図】　図1



【特許請求の範囲】
【請求項１】
内部ネットワークへの不正なアクセスを制限するファイアウォール装置において、
前記内部ネットワークに対する不正なアクセスを制限する外部ネットワークに接続されたファイアウォール手段と、
このファイアウォール手段を介して前記外部ネットワークに接続され前記ファイアウォール手段の設定の変更内容を取り込む設定インターフェイス手段と、
この設定インターフェイス手段を介して予め登録されている利用を許可された利用者であるかの認証をし、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性を評価した上で前記ファイアウォール手段の設定を変更する設定変更手段と
を備えたことを特徴とするファイアウォール装置。
【請求項２】
前記設定インターフェイス手段が、
ＷＷＷサーバであることを特徴とする
請求項１記載のファイアウォール装置。
【請求項３】
前記設定インターフェイス手段が、
ｔｅｌｎｅｔサーバであることを特徴とする
請求項１記載のファイアウォール装置。
【請求項４】
前記設定変更手段が、
利用者端末からアクセスがあった場合に利用者の認証処理を行い、
予め登録されている利用者であると判断した場合には予め登録されている認証された利用者の利用者情報に基づき設定可能な設定項目を制限し、
前記ファイアウォール手段の当該設定項目の設定状況を調査し、
設定可能な設定項目の設定状況を前記利用者端末に送信し、
前記利用者端末から受信した変更内容の正当性が認められれば前記ファイアウォール手段に対して受信した変更内容を反映させることを特徴とする
請求項１記載のファイアウォール装置。
【請求項５】
前記設定変更手段が、
設定変更の有効期限が満了した場合に前記ファイアウォール手段の設定を復元することを特徴とする
請求項１若しくは請求項４記載のファイアウォール装置。
【請求項６】
前記設定変更手段が、
予めデフォルトで設定されている有効期限を用いて前記ファイアウォール手段の設定を復元することを特徴とする
請求項１若しくは請求項４記載のファイアウォール装置。
【請求項７】
前記設定変更手段が、
変更内容に付加された設定変更の有効期限を用いて前記ファイアウォール手段の設定を復元することを特徴とする
請求項１若しくは請求項４記載のファイアウォール装置。
【請求項８】
前記設定変更手段が、
変更内容に付加された設定変更の有効期限が存在する場合には、付加された有効期限を用い、付加されていない場合には予めデフォルトで設定されている有効期限を用いて前記ファイアウォール手段の設定を復元することを特徴とする
請求項１若しくは請求項４記載のファイアウォール装置。

【請求項９】
前記設定変更手段が、
設定変更、若しくは、設定復元の内容を履歴として記憶手段に格納することを特徴とする請求項１，４，５，６，７若しくは請求項８のいずれかに記載のファイアウォール装置。
【請求項１０】
前記ファイアウォール手段が、
前記設置変更手段からの設定状況の照会があった場合には前記設定変更手段に対して設定状況を送信し、
前記設定変更手段から設定変更の要求があった場合には設定を変更し、
前記設定変更手段から設定復元の要求があった場合には設定を復元することを特徴とする請求項１記載のファイアウォール装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、内部ネットワークへの不正なアクセスを制限するファイアウォール装置に関し、特に誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能なファイアウォール装置に関する。
【０００２】
【従来の技術】
従来のファイアウォール装置は内部ネットワークとインターネット等の外部ネットワークとの間に設けられて、当該ファイアウォール装置を通過するデータを全て監視して内部ネットワークに対する不正なアクセスを制限するものである。
【０００３】
図６はこのような従来のファイアウォール装置の一例を用いたネットワークシステムを示す構成ブロック図である。図６において１は利用者端末、２はファイアウォール装置、３は管理者端末、１００はインターネット等の外部ネットワーク、１０１はイントラネット等の内部ネットワークである。
【０００４】
利用者端末１は外部ネットワーク１００を介してファイアウォール装置２に接続され、ファイアウォール装置２は内部ネットワーク１０１に接続される。また、管理者端末３もまた内部ネットワーク１０１に接続される。
【０００５】
また、図７はファイアウォール装置２の具体例を示す構成ブロック図である。図７において２，１００及び１０１は図６と同一符号を付してあり、４は内部ネットワークに対する不正なアクセスを制限するファイアウォール手段、５はファイアウォール手段４の設定の変更内容を取り込むと共に設定変更を行うためのＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）サーバやｔｅｌｎｅｔ（遠隔地から遠隔操作を行う等の仮想端末プロトコル：以下、単にｔｅｌｎｅｔと呼ぶ。）サーバ等の設定インターフェイス手段である。
【０００６】
ファイアウォール手段４は外部ネットワーク１００に接続され、ファイアウォール手段４は内部ネットワーク１０１に接続されると共に設定インターフェイス手段５に接続される。
【０００７】
ここで、図６示す従来のファイアウォール装置を用いたネットワークシステムの動作を図８を用いて説明する。図８はネットワークシステムにおけるファイアウォール装置の一時的な設定変更の手順を説明するフロー図である。
【０００８】
図８中”Ｓ００１”において利用者は予めファイアウォール装置４の管理者から管理者権限を取得して、利用者端末１から当該管理者権限を用いてファイアウォール装置４の設定インターフェイス手段５にアクセスする。

【０００９】
例えば、ファイアウォール装置４の管理者権限としては、管理者用のユーザＩＤ及びパスワードそれ自体であったり、若しくは、利用者のユーザＩＤに対して管理者の権限を付与してもらうことである。
【００１０】
また、例えば、設定インターフェイス手段５がＷＷＷサーバであれば利用者端末１にインストールされた汎用のＷｅｂブラウザでアクセスし、設定インターフェイス手段５がｔｅｌｎｅｔサーバであれば利用者端末１にインストールされたｔｅｌｎｅｔクライアントソフト等を用いてアクセスする。
【００１１】
図８中”Ｓ００２”において利用者は設定インターフェイス手段５の機能を用いて利用者端末１から内部ネットワーク１０１にアクセスが可能になるようにファイアウォール手段４の設定を変更する。
【００１２】
例えば、利用者がＷｅｂブラウザやｔｅｌｎｅｔクライアントソフトによって利用者端末１の画面上に表示された設定画面等を操作して設定変更を行い、利用者端末１から内部ネットワーク１０１へのアクセスを可能にする。
【００１３】
そして、図８中”Ｓ００３”において利用者は利用者端末１からファイアウォール手段４を通過して内部ネットワーク１０１にアクセスする。
【００１４】
図８中”Ｓ００４”において利用者が内部ネットワーク１０１への必要なアクセスが完了したと判断した場合には、図８中”Ｓ００５”において利用者は設定インターフェイス手段５の機能を用いてファイアウォール手段４の設定を復元する。
【００１５】
例えば、利用者がＷｅｂブラウザやｔｅｌｎｅｔクライアントソフトによって利用者端末１の画面上に表示された設定画面等を操作して設定の復元を行い、利用者端末１から内部ネットワーク１０１へのアクセスを制限させる。
【００１６】
この結果、管理者権限により設定インターフェイス手段５にアクセスしてファイアウォール手段４の設定を変更することにより、アクセス制限の一時的な変更が可能になる。
【００１７】
【発明が解決しようとする課題】
しかし、図６及び図７に示す従来例では利用者に管理者権限を与えるため、設定可能な範囲はファイアウォール手段４に関連する項目のみに限定することができず、言い換えれば、設定インターフェイス５等のファイアウォール装置２の他の機能の設定変更も可能になってしまい、誤設定による動作不良やセキュリティの低下を招いてしまうと言った問題点があった。
【００１８】
また、ファイアウォール手段４の設定変更をする利用者が複数人いる場合に、どの設定変更がどの利用者によるものであるのかを識別することができず、セキュリティ上好ましくないと言った問題点があった。
【００１９】
また、従来例では利用者毎に設定可能な項目を制限することができないので利用者に関係のない項目まで設定変更される恐れがあり、セキュリティの低下を招いてしまうと言った問題点があった。
【００２０】
また、従来例では設定変更の内容の正当性を判断していないので誤設定による動作不良やセキュリティの低下を招いてしまうと言った問題点があった。
【００２１】

さらに、ファイアウォール手段４のアクセス制限の一時的な解除（変更）は利用者が設定の復元を行うまで解消されないので、万が一、利用者が設定の復元を忘れた場合にはセキュリティホールとなる恐れがあり、セキュリティの低下を招いてしまうと言った問題点があった。
従って本発明が解決しようとする課題は、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能なファイアウォール装置を実現することにある。
【００２２】
【課題を解決するための手段】
このような課題を達成するために、本発明のうち請求項１記載の発明は、
内部ネットワークへの不正なアクセスを制限するファイアウォール装置において、
前記内部ネットワークに対する不正なアクセスを制限する外部ネットワークに接続されたファイアウォール手段と、このファイアウォール手段を介して前記外部ネットワークに接続され前記ファイアウォール手段の設定の変更内容を取り込む設定インターフェイス手段と、この設定インターフェイス手段を介して予め登録されている利用を許可された利用者であるかの認証をし、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性を評価した上で前記ファイアウォール手段の設定を変更する設定変更手段とを備えたことにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。
【００２３】
請求項２記載の発明は、
請求項１記載の発明であるファイアウォール装置において、
前記設定インターフェイス手段が、
ＷＷＷサーバであることにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。
【００２４】
請求項３記載の発明は、
請求項１記載の発明であるファイアウォール装置において、
前記設定インターフェイス手段が、
ｔｅｌｎｅｔサーバであることにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。
【００２５】
請求項４記載の発明は、
請求項１記載の発明であるファイアウォール装置において、
前記設定変更手段が、
利用者端末からアクセスがあった場合に利用者の認証処理を行い、予め登録されている利用者であると判断した場合には予め登録されている認証された利用者の利用者情報に基づき設定可能な設定項目を制限し、前記ファイアウォール手段の当該設定項目の設定状況を調査し、設定可能な設定項目の設定状況を前記利用者端末に送信し、前記利用者端末から受信した変更内容の正当性が認められれば前記ファイアウォール手段に対して受信した変更内容を反映させることにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。
【００２６】
請求項５記載の発明は、
請求項１若しくは請求項４記載の発明であるファイアウォール装置において、
前記設定変更手段が、
設定変更の有効期限が満了した場合に前記ファイアウォール手段の設定を復元することにより、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。
【００２７】
請求項６記載の発明は、

請求項１若しくは請求項４記載の発明であるファイアウォール装置において、
前記設定変更手段が、
予めデフォルトで設定されている有効期限を用いて前記ファイアウォール手段の設定を復元することにより、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。

【００２８】

請求項７記載の発明は、
請求項１若しくは請求項４記載の発明であるファイアウォール装置において、
前記設定変更手段が、
変更内容に付加された設定変更の有効期限を用いて前記ファイアウォール手段の設定を復元することにより、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。

【００２９】

請求項８記載の発明は、
請求項１若しくは請求項４記載の発明であるファイアウォール装置において、
前記設定変更手段が、
変更内容に付加された設定変更の有効期限が存在する場合には、付加された有効期限を用い、付加されていない場合には予めデフォルトで設定されている有効期限を用いて前記ファイアウォール手段の設定を復元することにより、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。

【００３０】

請求項９記載の発明は、
請求項１，４，５，６，７若しくは請求項８のいずれかに記載の発明であるファイアウォール装置において、
前記設定変更手段が、
設定変更、若しくは、設定復元の内容を履歴として記憶手段に格納することにより、設定変更等がどの利用者によるものであるのかを特定することが可能になる。

【００３１】

請求項１０記載の発明は、
請求項１記載の発明であるファイアウォール装置において、
前記ファイアウォール手段が、
前記設置変更手段からの設定状況の照会があった場合には前記設定変更手段に対して設定状況を送信し、前記設定変更手段から設定変更の要求があった場合には設定を変更し、前記設定変更手段から設定復元の要求があった場合には設定を復元することにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。

【００３２】

【発明の実施の形態】

以下本発明を図面を用いて詳細に説明する。図１は本発明に係るファイアウォール装置の一実施例を用いたネットワークシステムを示す構成ブロック図である。

【００３３】

図１において６は利用者端末、７はファイアウォール装置、８は管理者端末、１００ａはインターネット等の外部ネットワーク、１０１ａはイントラネット等の内部ネットワークである。

【００３４】

利用者端末６は外部ネットワーク１００ａを介してファイアウォール装置７に接続され、ファイアウォール装置７は内部ネットワーク１０１ａに接続される。また、管理者端末８もまた内部ネットワーク１０１ａに接続される。

【００３５】

また、図２はファイアウォール装置７の具体例を示す構成ブロック図である。図２において７，１００ａ及び１０１ａは図１と同一符号を付してあり、９は内部ネットワークに対

する不正なアクセスを制限するファイアウォール手段、１０はファイアウォール手段９の設定の変更内容を取り込むためのＷＷＷサーバやｔｅｌｎｅｔサーバ等の設定インターフェイス手段、１１はユーザ認証や正当性の判断等を行いファイアウォール手段９の設定変更を行う設定変更手段、１２は変更履歴等が格納される記憶手段である。

【００３６】

ファイアウォール手段９は外部ネットワーク１００ａに接続され、ファイアウォール手段９は内部ネットワーク１０１ａに接続されると共に及び設定インターフェイス手段１０に接続される。

【００３７】

また、設定変更手段１１の２つの入出力の内、一方の入出力が設定インターフェイス手段１０に接続され、他方の入出力がファイアウォール手段９に接続される。さらに、設定変更手段１１の出力が記憶手段１２に接続される。

【００３８】

ここで、図１示す実施例であるファイアウォール装置７を用いたネットワークシステムの動作を図３、図４及び図５を用いて説明する。図３はネットワークシステムにおける利用者端末６の動作を説明するフロー図、図４は設定変更手段１１の動作を説明するフロー図、図５はファイアウォール手段９の動作を説明するフロー図である。

【００３９】

設定変更手段１１には予め管理者により利用を許可する利用者の認証情報及び利用者情報が登録されている。

【００４０】

例えば、認証情報としては利用者毎に設定されたユーザＩＤ及びパスワード等であり、利用者情報としては当該利用者がファイアウォール手段９に対して変更可能な項目等である。

【００４１】

図３中”Ｓ１０１”において利用者端末６は設定インターフェイス手段１０を介して設定変更手段１１に接続する。そして、図３中”Ｓ１０２”において利用端者末６は利用者が入力した認証情報を設定インターフェイス手段１０を介して設定変更手段１１に送信する。

【００４２】

図３中”Ｓ１０３”において利用者端末６は設定インターフェイス手段１０を介して設定変更手段１１からファイアウォール手段９の設定状況を受信したか否かを判断し、もし、設定状況を受信した場合には図３中”Ｓ１０４”において設定状況を利用者端末６の表示手段に表示させる。

【００４３】

図３中”Ｓ１０５”において利用者端末６は設定インターフェイス手段１０の機能を用いてファイアウォール手段９の設定の変更をする。言い換えれば、設定の変更内容を設定インターフェイス手段１０を介して設定変更手段１１に送信する。この時、利用者端末６は同時に当該設定変更の有効期限を変更内容に付加して送信する。

【００４４】

例えば、利用者はＷｅｂブラウザやｔｅｌｎｅｔクライアントソフトによって利用者端末６の画面上に表示された設定画面等を操作して設定の変更を行い、利用者端末６から内部ネットワーク１０１ａへのアクセスを可能にする変更内容を設定インターフェイス手段１０を介して設定変更手段１１に送信する。

【００４５】

図３中”Ｓ１０６”において利用者端末６は設定インターフェイス手段１０を介して設定変更手段１１から設定変更が完了した旨の通知を受信したか否かを判断し、もし、設定変更の完了通知を受信した場合には図３中”Ｓ１０７”においてファイアウォール手段９を介して内部ネットワーク１０１ａにアクセスする。

【００４６】

一方、図４中”Ｓ２０１”において設定変更手段１１は設定インターフェイス手段１０を介して利用者端末６からのアクセスがあったか否かを判断する。もし、利用者端末６からのアクセスがあった場合には図４中”Ｓ２０２”において利用者の認証処理を行う。

【００４７】

例えば、設定変更手段１１はアクセスのあった利用者端末６のＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）アドレス等の必要な情報を取得すると共に利用者端末６から送信されてきた認証情報を受信し、予め登録されている利用を許可する利用者であるか否かを確認する。

【００４８】

そして、図４中”Ｓ２０３”において設定変更手段１１は受信した認証情報から予め登録されている利用者でないと判断した場合には、図４中”Ｓ２０１”のステップに戻る。

【００４９】

もし、図４中”Ｓ２０３”において設定変更手段１１は受信した認証情報から予め登録されている利用者であると判断した場合には、図４中”Ｓ２０４”において予め登録されている認証された利用者の利用者情報と、取得したＩＰアドレスとに基づき認証された利用者が設定可能な設定項目を決定し、言い換えれば、設定項目を制限し、ファイアウォール手段９の当該設定項目の設定状況を調査する。

【００５０】

図４中”Ｓ２０５”において設定変更手段１１は設定インターフェイス手段１０を介して認証された利用者が設定可能な設定項目と、調査結果である設定可能な設定項目の設定状況を利用者端末６に送信する。

【００５１】

そして、図４中”Ｓ２０６”において設定変更手段１１は利用者端末６からの設定の変更内容を受信するまで待機する。

【００５２】

図４中”Ｓ２０７”において設定変更手段１１は受信した変更内容の正当性を評価し、変更内容に矛盾や問題点等がなければ、言い換えれば、正当性が認められればファイアウォール手段９に対して受信した変更内容を反映させる。

【００５３】

例えば、受信した変更内容が”利用者端末６から内部ネットワーク１０１ａへのアクセスを可能にする”内容であった場合、設定変更手段１１はファイアウォール手段９に対して利用者端末６から内部ネットワーク１０１ａへのアクセスを許可させる。

【００５４】

もし、図４中”Ｓ２０７”において設定変更手段１１は受信した変更内容の正当性を評価し、変更内容に矛盾や問題点等があれば、設定変更手段１１は設定インターフェイス手段１０を介して利用者端末６に警告を与える。

【００５５】

例えば、設定変更手段１１は取得した利用者端末６のＩＰアドレスが”１０．０．ｘｘ．１０５”であるのに、変更内容に記載された内部ネットワーク１０１へのアクセスを許可させるＩＰアドレスが”１０．０．ｘｘ．１５”である場合には誤入力の可能性が高いのでその旨利用者端末６に警告を与える。

【００５６】

図４中”Ｓ２０８”において設定変更手段１１は設定変更の内容を履歴として記憶手段１２に格納する。例えば、日時、認証された利用者のユーザＩＤ、変更内容等を履歴として記憶手段１２に記録しておく。

【００５７】

図４中”Ｓ２０９”において設定変更手段１１は設定インターフェイス手段１０を介して設定変更が完了した旨の通知を利用者端末６に対して送信する。

【００５８】

図４中”Ｓ２１０”において設定変更手段１１は設定変更完了から時間が、受信した変更

内容に付加されていた有効期限を超過するまで待機し、言い換えれば、設定変更の有効期限が満了するまで待機する。

【００５９】

設定変更の有効期限が満了した場合、図４中”Ｓ２１１”において設定変更手段１１はファイアウォール手段９に対して設定を元の状態に復元し、図４中”Ｓ２１２”において設定の復元の内容を履歴として記憶手段１２に格納する。例えば、日時、認証された利用者のユーザＩＤ、復元内容等を履歴として記憶手段１２に記録しておく。

【００６０】

また、図５中”Ｓ３０１”においてファイアウォール手段９は設定変更手段１１からの設定状況の照会があったか否かを判断し、もし、設定状況の照会があった場合には図５中”Ｓ３０２”において設定変更手段１１に対して設定状況を送信して図５中”Ｓ３０１”に示すステップに戻る。

【００６１】

もし、図５中”Ｓ３０１”において設定状況の照会が無かった場合には、図５中”Ｓ３０３”においてファイアウォール手段９は設定変更手段１１から設定変更の要求があったか否かを判断し、もし、設定変更の要求があった場合には設定を変更して図５中”Ｓ３０１”に示すステップに戻る。

【００６２】

もし、図５中”Ｓ３０３”において設定変更の要求が無かった場合には、図５中”Ｓ３０５”においてファイアウォール手段９は設定変更手段１１から設定復元の要求があったか否かを判断し、もし、設定復元の要求があった場合には設定を復元して図５中”Ｓ３０１”に示すステップに戻る。

【００６３】

もし、図５中”Ｓ３０５”において設定復元の要求が無かった場合には、図５中”Ｓ３０１”に示すステップに戻る。

【００６４】

この結果、設定変更手段１１がユーザ認証を行い、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性を評価した上でファイアウォール手段９の設定を変更することにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。

【００６５】

また、設定変更手段１１がファイアウォール手段９の設定変更及び設定復元の内容を履歴として記憶手段１２に格納することにより、設定変更等がどの利用者によるものであるのかを特定することが可能になる。

【００６６】

さらに、設定変更手段１１が設定変更の有効期限が満了した場合に設定を復元することにより、万が一、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。

【００６７】

なお、図１に示す実施例を用いたネットワークシステムでは外部ネットワーク１００ａに接続された利用者端末６からのファイアウォール手段９の設置変更について説明しているが、勿論、内部ネットワーク１０１ａに接続された利用者端末からであっても同様にファイアウォール手段９の設定変更が可能である。

【００６８】

また、図３の説明に際しては利用者端末６が設定変更の有効期限を変更内容に付加して送信する旨例示されているが、設定変更手段１１が予めデフォルトで設定されている有効期限を使用しても良い。

【００６９】

さらに、設定変更手段１１が利用者端末６から変更内容に付加された設定変更の有効期限が存在する場合には、付加された有効期限を用い、付加されていない場合には予めデフォ

ルトで設定されている有効期限を用いても良い。

【００７０】

これらの場合には、利用者端末６が設定変更の有効期限を変更内容に付加して送信する必要性がなくなるので、有効期限の付加し忘れによるセキュリティの低下を防止することができる。

【００７１】

また、図２に示す設定変更手段１１の機能をネットワークルータに具備させることにより、ネットワークルータに適用することが可能になる。

【００７２】

また、図２に示す設定変更手段１１の機能をファイアウォール・ソフトウェアに具備させることにより、ファイアウォール・ソフトウェアに適用することが可能になる。

【００７３】

また、図２に示す設定変更手段１１の機能をネットワークルータ管理ソフトウェアに具備させることにより、ネットワークルータ管理ソフトウェアに適用することが可能になる。

【００７４】

また、図４に示す設定変更手段の動作説明では認証された利用者の利用者情報と取得したＩＰアドレスに基づき認証された利用者が設定可能な設定項目を制限している旨例示されているが、認証された利用者の利用者情報のみに基づき認証された利用者が設定可能な設定項目を制限しても構わない。

【００７５】

【発明の効果】

以上説明したことから明らかなように、本発明によれば次のような効果がある。

請求項１，２，３，４及び請求項１０の発明によれば、設定変更手段がユーザ認証を行い、認証された利用者毎に設定可能な設定項目を制限し、変更内容の正当性を評価した上でファイアウォール手段の設定を変更することにより、誤設定やセキュリティの低下を招くことなくアクセス制限の一時的な変更が可能になる。

【００７６】

また、請求項５，６，７及び請求項８の発明によれば、設定変更手段が設定変更の有効期限が満了した場合に設定を復元することにより、万が一、利用者が設定の復元を忘れた場合であってもセキュリティホールとはならず、セキュリティの低下を防止することができる。

【００７７】

また、請求項９の発明によれば、設定変更手段がファイアウォール手段の設定変更及び設定復元の内容を履歴として記憶手段に格納することにより、設定変更等がどの利用者によるものであるのかを特定することが可能になる。

【図面の簡単な説明】

【図１】本発明に係るファイアウォール装置の一実施例を用いたネットワークシステムを示す構成ブロック図である。

【図２】ファイアウォール装置の具体例を示す構成ブロック図である。

【図３】ネットワークシステムにおける利用者端末の動作を説明するフロー図である。

【図４】設定変更手段の動作を説明するフロー図である。

【図５】ファイアウォール手段の動作を説明するフロー図である。

【図６】従来のファイアウォール装置の一例を用いたネットワークシステムを示す構成ブロック図である。

【図７】ファイアウォール装置の具体例を示す構成ブロック図である。

【図８】ネットワークシステムにおけるファイアウォール装置の一時的な設定変更の手順を説明するフロー図である。

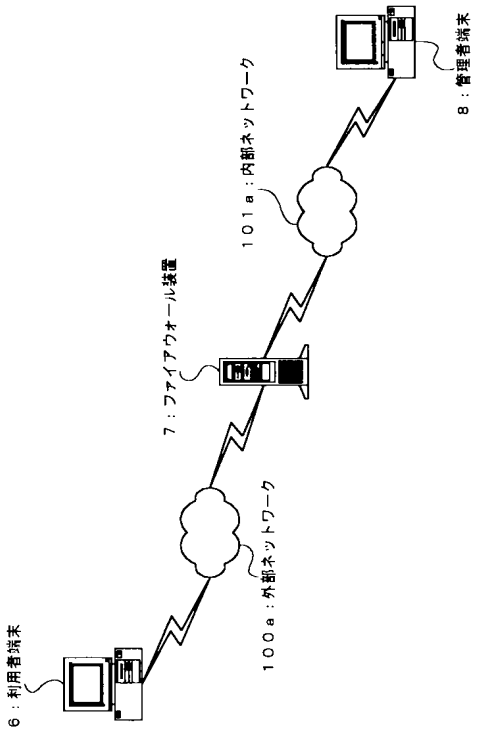
【符号の説明】

１，６　利用者端末

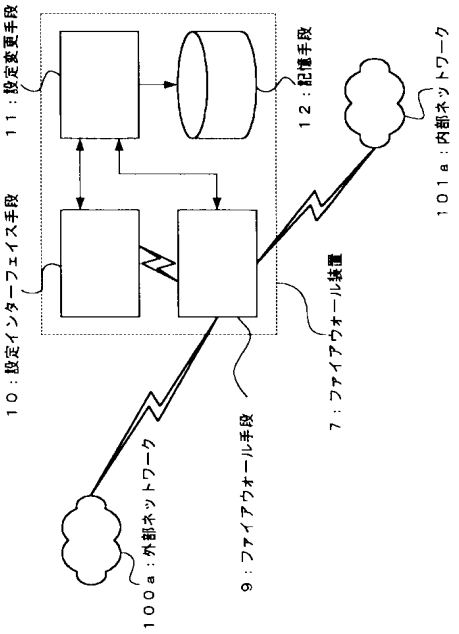
２，７　ファイアウォール装置

３，８　管理者端末
４，９　ファイアウォール手段
５，１０　設定インターフェイス手段
１１　設定変更手段
１２　記憶手段
１００，１００ａ　外部ネットワーク
１０１，１０１ａ　内部ネットワーク

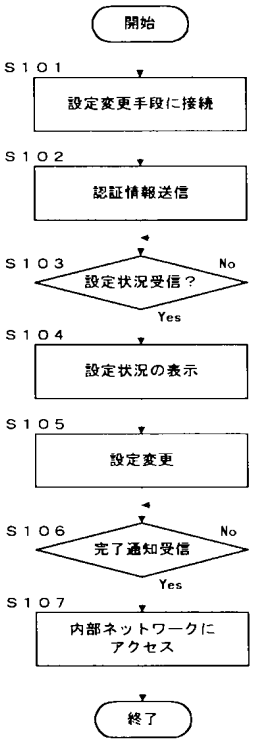
【図１】



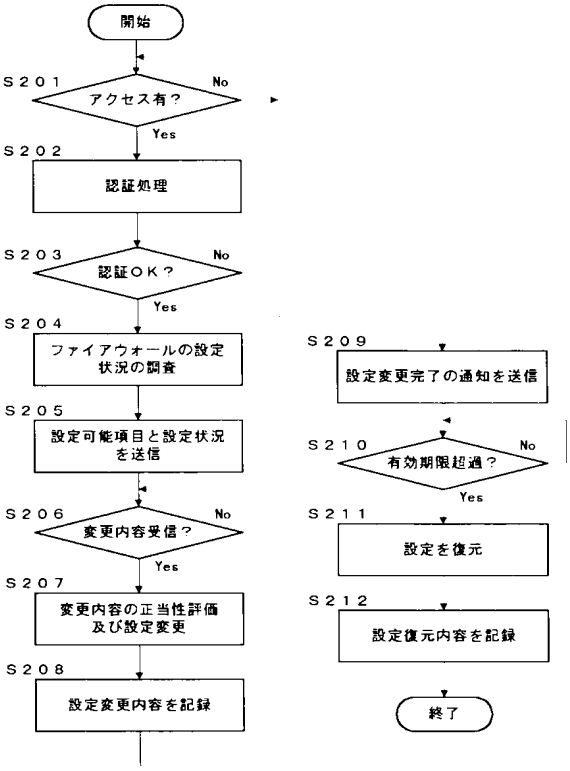
【図２】



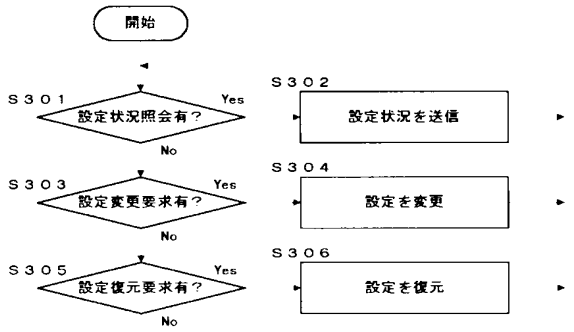
【図３】


開始
S101
設定変更手段に接続
S102
認証情報送信
S103
設定状況受信？
No
Yes
S104
設定状況の表示
S105
設定変更
S106
完了通知受信
No
Yes
S107
内部ネットワークにアクセス
終了

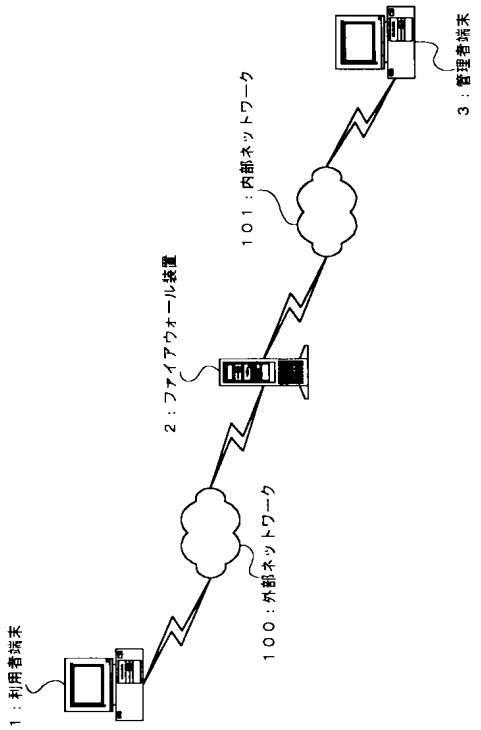
【図４】


開始
S201
アクセス有？
No
Yes
S202
認証処理
S203
認証ＯＫ？
No
Yes
S204
ファイアウォールの設定状況の調査
S205
設定可能項目と設定状況を送信
S206
変更内容受信？
No
Yes
S207
変更内容の正当性評価及び設定変更
S208
設定変更内容を記録
S209
設定変更完了の通知を送信
S210
有効期限超過？
No
Yes
S211
設定を復元
S212
設定復元内容を記録
終了

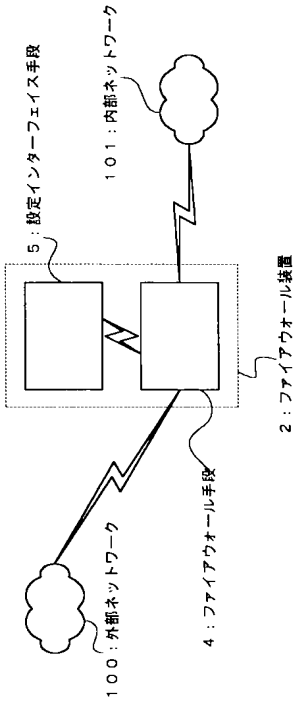
【図５】


開始
S301
設定状況照会有？
Yes
No
S302
設定状況を送信
S303
設定変更要求有？
Yes
No
S304
設定を変更
S305
設定復元要求有？
Yes
No
S306
設定を復元

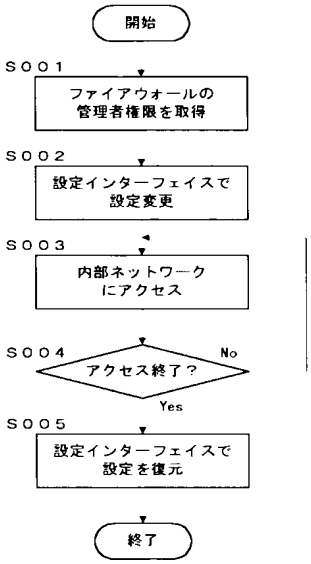
【図６】


3：管理者端末
101：内部ネットワーク
2：ファイアウォール装置
100：外部ネットワーク
1：利用者端末

【図７】


５：設定インターフェイス手段
１０１：内部ネットワーク
２：ファイアウォール装置
４：ファイアウォール手段
１００：外部ネットワーク

【図８】


開始
S001
ファイアウォールの
管理者権限を取得
S002
設定インターフェイスで
設定変更
S003
内部ネットワーク
にアクセス
S004
アクセス終了？
No
Yes
S005
設定インターフェイスで
設定を復元
終了